Cyberbullying and Cyberthreats

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org and http://cyberbully.org
E-mail: nwillard@csriu.org

Cyberbullying

Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies.

Cyberbullying can take different forms, including:

- Flaming. Online "fights" using electronic messages with angry and vulgar language.
  - Joe and Alec's online fight got angrier and angrier. Insults were flying. Joe warns Alec to watch his back in school the next day.
- Harassment. Repeatedly sending offensive, rude, and insulting messages.
  - Matt reported to the principal that students were bullying another student. When Matt got home, he had 35 angry messages in her email box. The anonymous cruel messages kept coming—some from total strangers.
  - A group of girls at his school had been taunting Alan through instant messaging, teasing him about his small size, daring him to do things he couldn't do, suggesting the world would be a better place if he committed suicide. One day, he shot himself. His last online message was, "Sometimes the only way to get the respect you deserve is to die."
- Denigration. "Dissing" someone online. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships.
  - Brad's blog is filled with racist profanity. Frequently, he targets black and Latino student leaders, as well as minority teachers, in his angry verbal assaults.
  - Middle school students created a web site denigrating Raymond. They posted stories, jokes, and cartoons ridiculing his size and questioning his sexuality.
  - Sue was really angry at Kelsey, who she thought stole her boyfriend. Sue convinced Marilyn to post anonymous comments on a discussion board slamming Kelsey. Marilyn was eager to win Sue's approval and fit into her group of friends, so she did as Sue requested.
- Impersonation. Breaking into someone's account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person's reputation or friendships.
  - Laura watched closely as Emma logged on to her account and discovered her password. Later, Laura logged on to Emma's account and sent a scathing message to Emma's boyfriend, Adam.
- Outing and Trickery. Sharing someone's secrets or embarrassing information or images online. Tricking someone into revealing secrets or embarrassing information, which is then shared online.
  - Sitting around the computer with her friends, Judy asked, "Who can we mess with?" Judy started IM-ing with Sara, asking her many personal questions. The next day, the girls were passing around Sara's IM at school.
  - Greg, an obese high school student, was changing in the locker room after gym class. Matt took a covert picture of him with his cell phone camera. Within seconds, the picture was flying around the cell phones at school.
- Exclusion. Intentionally excluding someone from an online group, like a "buddy list."

- Millie tries hard to fit in with group of girls at school. She recently got on the “outs” with a leader in this group. Now Millie has been excluded from the IM “buddy” lists of all of the girls.

- Cyberstalking. Repeatedly sending messages that include threats of harm or are highly intimidating. Engaging in other online activities that make a person afraid for her or her safety.
  - When Annie broke up with Sam, he sent her many angry, threatening, pleading messages. He spread nasty rumors about her to her friends and posted a sexually suggestive picture she had given him in a sex-oriented discussion group, along with her email address and cell phone number.

Cyberthreats

Cyberthreats are either direct threats or distressing material that raises concerns or provides clues that the person is emotionally upset and may be considering harming someone, harming him or herself, or committing suicide.

- Joe and Alec’s online fight got angrier and angrier. Insults were flying. Joe warns Alec to watch his back in school the next day.
- Jeff comments in his blog: "I'm a retarded [expletive] for ever believing that things would change. I'm starting to regret sticking around. It takes courage to turn the gun on your self, takes courage to face death.” Later he wrote: “Things are kind of rocky right now so I might disappear unexpectedly.
- Celia met Andrew in a chat room. Andrew wrote: “bring a gun to school, ur on the front of every … i cant imagine going through life without killing a few people … people can be kissing my shotgun straight out of doom … if i dont like the way u look at me, u die … i choose who lives and who dies”

How, Who, and Why

- Cyberbullying or cyberthreat material—text or images—may be posted on personal web sites or blogs or transmitted via email, discussion groups, message boards, chat, IM, or cell phones.
- A cyberbully may be a person whom the target knows or an online stranger. Or the cyberbully may be anonymous so it is not possible to tell. A cyberbully may solicit involvement of other people who do not know the target—cyberbullying-by-proxy.
- Cyberbullying and cyberthreats may be related to in-school bullying. Sometimes, the student who is victimized at school is also being bullied online. But other times, the person who is victimized at school becomes a cyberbully and retaliates online. Other times, the student who is victimized will share his or her anger or depression online as distressing material.
- It appears that the students most often involved in cyberbullying are the “in-crowd” students, with the “wannabes” the most frequent targets.
- Cyberbullying may involve relationships. If a relationship breaks up, one person may start to cyberbully the other person. Other times, teens may get into online fights about relationships.
- Cyberbullying may be based on hate or bias—bullying others because of race, religion, obesity, or sexual orientation.
- Teens may think that cyberbullying entertaining—a game to hurt other people.
- Teens may have no one to talk with about how bad they are feeling and how horrible their life is. So they describe this online. They might think that if they post this material online, they will meet someone who cares about them. Unfortunately, they may meet a dangerous stranger or hook up with other hurt teens who only reinforce their bad feeling.
- Youth make threats all of the time. Their tone of voice, posture, overall interaction allow others to determine whether or not expression is a “real threat. Online material that looks threatening could be:
  - A joke, parody, or game.
  - A rumor that got started and has grown and spread.

- Material posted by a young person who is trying out a fictitious threatening online character.
- The final salvos of a “flame war” that has gotten out of hand, but will unlikely result in any real violence.
- Material posted by someone impersonating another someone else for the purpose of getting that person into trouble.
- Distressing material posted by a depressed or angry young person that could foretell a violent or suicidal intention, but does not represent an imminent threat.
- A legitimate imminent threat. ”

- "Leakage" occurs when a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act. Schools should assume that emotional distraught youth with Internet access will be posting material that provides significant insight into their mental state
  - We must learn how to find, analyze, and effectively respond to cyberthreats.
  - We must specifically encourage youth to identify and report cyberthreats.

The Impact of Cyberbullying

It is widely known that face-to-face bullying can result in long-term psychological harm to targets. This harm includes low self-esteem, depression, anger, school failure, school avoidance, and, in some cases, school violence or suicide. It is possible that the harm caused by cyberbullying may be even greater than harm caused by traditional bullying because...

- Online communications can be extremely vicious.
- There is no escape for those who are being cyberbullied—victimization is ongoing, 24/7.
- Cyberbullying material can be distributed worldwide and is often irretrievable.
- Cyberbullies can be anonymous and can solicit the involvement of unknown “friends.”
- Teens may be reluctant to tell adults what is happening online or through their cell phone because they are emotionally traumatized, think it is their fault, fear greater retribution, or fear online activities or cell phone use will be restricted.

Cyberbullying: Bully, Target, and Bystander

If students have been actively socializing online, it is probable that they have been involved in cyberbullying in one or more of the following roles:

- Bullies. “Put-downers” who harass and demean others, especially those they think are different or inferior, or “get-backers” who have been bullied by others and are using the Internet to retaliate or vent their anger.
- Targets. The targets of the cyberbully.
- Harmful Bystanders. Those who encourage and support the bully or watch the bullying from the sidelines, but do nothing to intervene or help the target.
- Helpful Bystanders. Those who seek to stop the bullying, protest it, provide support to the target, or tell an adult. We need more of these kinds of bystanders!

You Can’t See Me. I Can’t See You

Why is it that when people use the Internet or other technologies, they sometimes do things that they would never do in the “real world?” Here are some of the reasons:

- You Can’t See Me. When people use the Internet, they perceive they are invisible. The perception can be enhanced because they create anonymous accounts. People are not really invisible, because online activities can be traced. But if you think you are invisible, this removes concerns of detection, disapproval, or punishment.
- I Can’t See You. When people use the Internet they do not receive tangible feedback about the consequences of their actions, including actions that have hurt someone. Lack of feedback interferes with empathy and leads to the misperception that no harm has resulted.
- Everybody Does It. The perception of invisibility and lack of tangible feedback support risky or irresponsible online social norms, including:

- "Life online is just a game." Allows teens to ignore the harmful "real world" consequences of online actions and creates the expectation that others will simply blow off any online harm.
- "Look at me—I'm a star." Supports excessive disclosure of intimate information and personal attacks on others, which is generally done for the purpose of attracting attention.
- "It's not me. It's my online persona." Allows teens to deny responsibility for actions taken by one of their online personas or identities.
- "What happens online, stays online." Supports the idea that one should not bring issues related to what has happened online into the "real world" and should not disclose online activity to adults.
- "On the Internet, I have the free speech right to write or post anything I want regardless of the harm it might cause to another." Supports harmful speech and cruel behavior as a free speech right.

Limits

We need to educate students about the limits on "free speech."

- Family values.
- School rules.
- Terms of use agreements of Internet service providers, web sites, and cell phone companies.
- Civil law standards. Cyberbullying could meet standards for:
  - Defamation.
  - Invasion of privacy by disclosure of private fact.
  - Intentional infliction of emotional distress.
- Criminal law. Cyberbullying could be in violation of criminal law:
  - Threats of violence.
  - Harassment or stalking.
  - Hate or bias crimes.
  - Material harmful to minors, child pornography, or sexual exploitation.
  - Taking photo in private place.
  - Personal values.

Legal Issues

<u>Search and seizure</u>

When can a school monitor and search student Internet use records and files?

Apply the "locker standard" to Internet use.

- Users have a limited expectation of privacy on the district's Internet system.
- Routine maintenance and monitoring, (technical and by staff) may lead to discovery that a user has violated district policy or law.
- An individual search will be conducted if there is reasonable suspicion that a user has violated district policy or the law.
- Schools should determine who has authority to authorize individual search and record-keeping.

Clear notice can enhance deterrence.

<u>Free speech issues</u>

When can a school respond to cyberbullying?

The First Amendment places restrictions on public officials when intervening in situations involving expression of speech by students.

- Tinker standard. School officials may intervene only when there is a substantial and material threat of disruption or interference with the rights of other students. Has recently been applied to off-campus online speech by students that relates to the school. But some legal commentators disagree.
- Hazelwood standard. School officials may impose educationally-based restrictions.

- Applies to on-campus speech that occurs through a school-authorized forum, such as school newspaper. Should apply to speech disseminated through district Internet system and campus use of cell phones.
- Off-campus online harmful speech cases.
  - All but one case—speech directed at staff.
  - All cases—decided based on Tinker standard.
  - All but one case—the district settled or lost.
  - In one case — the district won because the student had accessed the site from school and the teacher was very emotionally upset.
  - No cases—addressing really serious harmful online speech directed at a student.
- If off-campus online speech of a student has caused a material and substantial disruption in the life of another student, can the school respond? Unknown.
- Will Tinker will continue to apply? Unknown.
- How can schools handle the unknowns?
  - Search diligently for, and document, school "nexus" to bring case under Hazelwood standard.
    - Material posted or sent through district Internet system.
    - Material displayed to other students through district Internet system.
    - Material originated on-campus.
    - Relationship with on-campus bullying.
  - If school "nexus" can't be found, support victim, contact parents to seek informal resolution, recommend civil litigation, or contact police.

<u>District liability</u>

When must a school respond to cyberbullying?

District liability concerns are raised when cyberbullying or cyberthreats are occurring through district Internet system or via cell phone on campus.

Negligence claim

- Duty to protect. Duty to anticipate foreseeable dangers and take necessary precautions
  - Schools have a duty to exercise precautions against student cyberbullying through district Internet system and through use of cell phones on campus.
- Failure to exercise a reasonable standard of care. How would a "reasonable" educator in a similar situation have acted? Has the district established a reasonable level of supervision/monitoring of student use of the Internet and provided a vehicle to report and respond to cyberbullying activity?
  - Many districts have not established a reasonable level of monitoring and do not have effective reporting/response.
- Proximate cause. Was the student's injury foreseeable? Was there as a connection between breach of duty and injury? Was it foreseeable that students could be using the district's Internet system to post to send harmful material to other students and did the lack of supervision/monitoring allow such an injury to occur?
  - It is entirely foreseeable that students are using the district Internet system to cyberbully others, whether there is a connection will depend on facts.
- Actual injury. Was there a physical/emotional injury?
  - Will depend on the facts.

Statutory liability

Civil rights statutes

- Title IX of the Education Amendments of 1972.
- Title VI of the Civil Rights Act of 1964.
- State civil rights statutes.
- A violation of Title IX and VI may be found if a school has effectively caused, encouraged, accepted, tolerated, or failed to correct a sexually or racially hostile environment of which it has actual or constructive notice.

- A school is charged with constructive notice of a hostile environment if, upon reasonably diligent inquiry in the exercise of reasonable care, it should have known of the discrimination.
- Is the district being reasonably diligent in ensuring that students are not using the district Internet system in a harmful manner?

Comprehensive School and Community-based Approach to Address Cyberbullying and Cyberthreats

Research-guided approach, based on:
- Best practices in bullying, violence, and suicide prevention programs.
- Research insight into bullying.
- Traditional threat assessment processes.
- Combined with:
  - Insight into online behavior of youth.
  - Legal analysis.
  - Comprehensive approach to manage Internet use in school and home.
- Not yet research-based. If using federal safe schools funds, must request waiver of Principles of Effectiveness

<u>Comprehensive planning through safe schools committee</u>
- Administrator.
- Counselor/psychologist.
- Technology director.
- Librarian.
- Community members. School security officer, parents, law enforcement, mental health organizations
- Students. Probably important, but potentially problematical because students could be viewed as traitors.

<u>Needs assessment—bringing "sunlight" to the problem</u>
- Student survey to address:
  - On-campus or off-campus instances.
  - Relationship to on-campus actions.
  - Impacts.
  - Reporting concerns.
  - Attitudes, risk factors, and protective factors.
- May need to be done first, to convince people that there is a real concern.

<u>Policy and practice review</u>
- Establish/expand bullying/threat report process.
- Anonymous and/or confidential because concerns about online retaliation are very real.
- Establish an online reporting form or email report.
- Review cell phone/PDA policies and practices.
- Misuse should lead to discipline for bullying and ban on device at school.
- Review Internet policies and practices.
- Establish cyberbully or cyberthreat situation review and threat assessment process.
- Overall threat assessment process must also address Internet communications – if any threat is made, search for additional material online.
- Establish cyberbullying intervention process.

<u>Professional development</u>
- "Triage" approach.
- Key person in district/region/state needs high level of training.
- Safe schools planning committee and all "first responders" need insight into problem and ways to detect, review, and intervene, with back-up from key person..
- All other staff need general awareness.

Parent and community outreach

- Provide information on how to:
  - Prevent, detect and intervene if child is victim.
  - Prevent child from being cyberbully.
  - Possible consequences if child is a cyberbully.
  - Strategies to empower and activate bystanders.
- Provide information to parents through:
  - General information through newsletters.
  - Parent workshops.
  - "Just-in-time" comprehensive resources in office and online because parents likely will not pay attention until they need the information.
- Provide information and training to others:
  - Mental health professionals.
  - Faith-based organizations.
  - Youth organizations.
  - Public library and community technology centers.
  - Media.

Student education

Prerequisite to addressing cyberbullying is effective social skills education.

- Educational approach should foster internalized values and character and empowerment of victims and bystanders.
- While it is necessary to improve monitoring and apply consequences, a behavior-management approach to education will not work because cyberbullying is occurring in online environments where there are no responsible adults.
- Enhance predictive empathy skills.
- Teach ethical decision-making skills.
- Teach conflict resolution and peer mediation.
- Enhance understanding of legal principles for online publishing.
- Address Internet privacy, public disclosure, and safety concerns.
- Provide encouragement for reporting cyberthreats.

Evaluation and assessment

- Ongoing evaluation is critically important.
- Cyberbullying is an emerging concern in a new environment that is not fully understood.
- Evaluation should inform implementation.
- Performance measures approach.
  - Performance objectives – tie to needs assessment findings.
  - Inputs — resources allocated to the activities.
  - Activities — specific program activities or tasks.
  - Outputs — direct products of the program activities.
  - Outcomes — consequences of the program on the intended recipients.

Cyberbully or Cyberthreat Situation Review

See attached.